UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/631,091	07/31/2003	Philip Kwan	019959-001610US	3218

20350 7590 07/24/2007
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
DADA, BEEMNET W	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
07/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/631,091	**Applicant(s)** KWAN, PHILIP	
	Examiner Beemnet W. Dada	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 14 May 2007.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-19 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-19 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on May 14, 2007. Claims 1-19 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1 and 3-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Rayes et al. US 7,234,163 B1 (hereinafter Rayes).

5. As per claims 1 and 15, Rayes teaches a method for detecting ARP spoofing including:

receiving an ARP reply on a port of a network device [column 7, lines 35-37];

generating a data packet, wherein the data packet includes information from the ARP reply, and an identification of the port on which the ARP reply was received [column 7, lines 35-44, line 63-column 8, line 3];

storing information contained in the data packet in a database of an ARP collector [column 7, line 63 – column 8, line 19]; and analyzing information in the database to determine when ARP spoofing occurs [column 7, line 63 – column 9, line 4].

6. As per claim 9, Rayes teaches an ARP collector method for detecting ARP spoofing, the method comprising:

receiving ATP packets from a first subnet of a computer network (i.e., from computer 140 A) [column 5, lines 41-50 and column 7, lines 35-41, and figure 1, units 140A, 160 &170];

receiving ATP packets from a second subnet of the computer network (i.e., from computer 140B) [column 5, lines 41-50 and column 7, lines 35-41, and figure 1, units 140A, 160 &170];

storing information from the ATP packets from the first subnet in database of the ARP collector [column 7, line 63 – column 8, line 19];

storing information from the ATP packets from the second subnet in the database of the ARP collector [column 7, line 63 – column 8, line 19]; and

analyzing received ATP packets and information in ARP collector database to determine when a spoofed ARP reply has been received on a port of the computer network [column 7, line 63 – column 9, line 4].

7. As per claim 3, Rayes further teaches the method wherein the information stored in the database includes MAC address of a device which generated an ARP reply and an IP address given as a source IP address in the ARP reply [figure 1, units 160 &170].

8. As per claims 4, 5 and 16, Rayes further teaches the method wherein the information stored in the database includes a MAC address of a device which generated an ARP reply, and

an IP address given as a source IP address in the ARP reply and a time at which the ARP reply was received on the port, and an identification of the port on which the ARP reply was received [figure 1, units 160 &170 and column 7, lines 13-21].

9. As per claims 6, 10 and 18, Rayes further teaches the method wherein when it is determined that there is a spoofed ARP reply, blocking the port on which the spoofed ARP reply was received [column 9, lines 20-42].

10. As per claims 7, 11 and 19, Rayes further teaches the method wherein when it is determined that there is a spoofed ARP reply, filtering a MAC address which generated the spoofed ARP reply at a port at which the spoofed ARP reply was received [column 9, lines 20-43].

11. As per claim 8 and 17, Rayes further teaches the method further comprising:

transmitting the data packet to the ARP collector and generating an alert when an ARP spoofing condition occurs [column 9, lines 6-19].

12. As per claims 12 and 13, Rayes further teaches the method wherein the ATP packets from the first subnet, and the ATP packets from the second subnet include ARP reply information received on ports of network devices in the respective subnets, and information in the ATP packets includes information identifying a port on which a particular ARP reply was received [figure 1, 140A, 140B, 137A, 137B, and column 5, lines 41-50 and column 7, lines 35-41].

13. As per claim 14, Rayes further teaches the method further including,

storing ARP reply information indicating a MAC address which is identified as a source of an ARP reply, storing ARP reply information indicating an IP address which is identified as a source of an ARP reply, and storing information indicating a port on which an ARP reply was received [column 7, line 63 – column 8, line 19 and figure 1].

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rayes et al. US 7,234,163 B1 (hereinafter Rayes) in view of Gunter et al. US 6,751,728 B1 (hereinafter Gunter).

16. As per claim 2, Rayes teaches a method of detecting ARP spoofing as indicated above. Rayes is silent on generating the data packet which includes encrypting the data packet. However, encrypting data packets is old and well known in the art which has the advantage of enhancing security of a system. For example, Gunter teaches transmitting packets, including encrypting the transmitted packets [see at least abstract]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Gunter within the system of Rayes in order to enhance security of the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

July 13, 2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100